PATENT ABSTRACTS OF JAPAN

(11)Publication number : **02-249333**
(43)Date of publication of application : **05.10.1990**

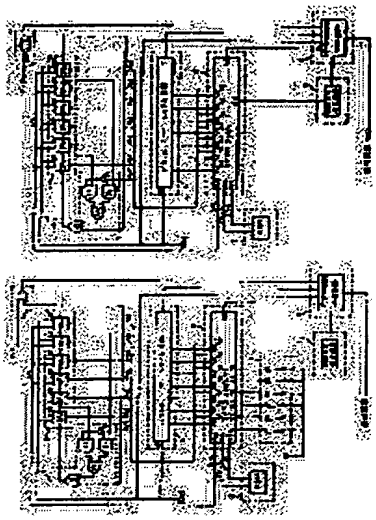
(51)Int.CI. **H04L 9/06**
H04L 9/14

(21)Application number : **01-070200**
(22)Date of filing : **22.03.1989**

(71)Applicant : **SHARP CORP**
(72)Inventor : **HIRAIDE JUNJI**
TADA JUNJI

(54) PRIVACY TELEPHONE SET

(57)Abstract:
PURPOSE: To eliminate the need for revision of a key in the case of revising a cipher by providing a pseudo random signal generating circuit, a storage circuit, a control means and a conversion circuit respectively to a transmission side and a reception side, providing a ciphering key setting means, a ciphering circuit to the transmission side and a decoding circuit to the reception side.
CONSTITUTION: First and 2nd pseudo random signal generating circuits 1, 2 at the transmission side an the reception side employ shift registers having a feedback path capable of switching and generate various different pseudo random signals by revising the feedback path and the initial value. On the other hand, 1st and 2nd storage circuits 3, 3 store the plural sets of initial values and feedback path setting data of the pseudo random signal generating circuits 1, 2, read the storage content of the storage circuit 3 in response to the setting of a ciphering key setting means 5 to set the pseudo ran dom signal generating circuits 1, 2, thereby generating different pseudo random signals. Then the reception side selects the pseudo random signal from the pseudo random signal generating circuits 1, 2 to make the pseudo random signal identical to the transmission side and the reception side. Thus, it is not required to replace the cipher ing key itself and the setting and revision of the key are attained easily and freely.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

⑲日本国特許庁（JP）　⑪特許出願公開

⑫公開特許公報（A）　平2－249333

⑤Int.Cl.⁵　識別記号　庁内整理番号　⑬公開　平成2年(1990)10月5日

H 04 L 9/06
9/14

6945－5K　H 04 L 9/02　Z

審査請求　未請求　請求項の数 1　（全5頁）

⑭発明の名称　秘話装置

⑳特　願　平1－70200

㉒出　願　平1(1989)3月22日

⑫発明者　平出　順二　大阪府大阪市阿倍野区長池町22番22号　シャープ株式会社内

⑫発明者　多田　順次　大阪府大阪市阿倍野区長池町22番22号　シャープ株式会社内

⑪出願人　シャープ株式会社　大阪府大阪市阿倍野区長池町22番22号

⑭代理人　弁理士　山口　邦夫

明　細　書

1．発明の名称

秘話装置

2．特許請求の範囲

（1）送信側は、

切り替え可能な帰還路を有するシフト・レジスタを用いた第1疑似ランダム信号発生回路と、

暗号鍵を設定する暗号鍵設定手段と、

上記疑似ランダム信号発生回路の初期値及び帰還路設定データを記憶した第1記憶回路と、

上記暗号鍵に応じて上記第1記憶回路から上記初期値及び帰還路設定データを読出し、上記第1疑似ランダム信号発生回路を設定する第1制御手段と、

上記暗号鍵に応じたパラレル・アドレス信号をシリアル・アドレス信号に変換する第1変換回路と、

上記第1疑似ランダム信号発生回路の出力信号により入力データを暗号化する暗号化回路とを具え、

該暗号化回路の出力データ及び上記シリアル・アドレス信号を送信し、

受信側は、

上記第1疑似ランダム信号発生回路と同じ構成の第2疑似ランダム信号発生回路と、

上記第1記憶回路と同じ内容を記憶した第2記憶回路と、

受信した上記シリアル・アドレス信号をパラレル・アドレス信号に変換する第2変換回路と、

該第2変換回路からのパラレル・アドレス信号により、上記第2記憶回路から上記初期値及び帰還路設定データを読出し、上記第2疑似ランダム信号発生回路を設定する第2制御手段と、

上記第2疑似ランダム信号発生回路の出力信号により、受信したデータを復号化する復号化回路とを具えたことを特徴とする秘話装置。

2．発明の詳細な説明

〔産業上の利用分野〕

本発明は、有線及び無線デジタル通信における秘話装置に関する。

[従来の技術]

有線及び無線通信において、通信内容が秘密の場合、秘話通信を行なう必要がある。そのために、送信側では、通常のデータ（平文）を暗号化して、有線又は無線の通信区間を暗号データ（暗号文）で通信する。そして、受信側にて、この暗号文を変換文に復号化する。

第４図は、従来の秘話装置を示す。送信側においては、暗号化回路１３が、暗号化鍵（暗号化を制御する手段）１５に応じて平文を暗号文に変換する。

暗号化回路１３からの暗号文は、有線又は無線の通信区間を介して、受信側に供給される。

受信側では、復号化回路１４が、復号化鍵（復号化を制御する手段）１６に応じて、暗号文を平文に変換する。

[発明が解決しようとする課題]

第４図に示した従来の秘話装置では、送信側及び受信側が、暗号化及び復号化のために、同一又は独立した鍵を所有する必要がある。これら鍵は、暗号に応じて予め定めておく必要があり、暗号を変更する際は、その度毎に、新たに鍵を取り決める必要がある。

よって、暗号の鍵を設定したり、変更するのが非常に煩わしかった。しかし、通信の秘密を確保するには、度々、暗号の鍵を変更する必要があった。

したがって、本発明の目的は、暗号を変更する際に、鍵を変更する必要がなく、暗号の設定及び変更が容易に行える秘話装置の提供にある。

[課題を解決するための手段]

本発明の秘話装置は、送信側と受信側とに別れている。

送信側は、切り替え可能な帰還路を有するシフト・レジスタを用いた第１疑似ランダム信号発生回路と、

暗号鍵を設定する暗号鍵設定手段と、

疑似ランダム信号発生回路の初期値及び帰還路設定データを記憶した第１記憶回路と、

暗号鍵に応じて第１記憶回路から初期値及び帰還路設定データを読出し、第１疑似ランダム信号発生回路を設定する第１制御手段と、

暗号鍵に応じたパラレル・アドレス信号をシリアル・アドレス信号に変換する第１変換回路と、

第１疑似ランダム信号発生回路の出力信号により入力データを暗号化する暗号化回路とを具えている。

そして、送信側は、暗号化回路の出力データ及びシリアル・アドレス信号を送信する。

また、受信側は、第１疑似ランダム信号発生回路と同じ構成の第２疑似ランダム信号発生回路と、

第１記憶回路と同じ内容を記憶した第２記憶回路と、

受信したシリアル・アドレス信号をパラレル・アドレス信号に変換する第２変換回路と、

この第２変換回路からのパラレル・アドレス信号により、第２記憶回路から初期値及び帰還路設定データを読出し、第２疑似ランダム信号発生回路を設定する第２制御手段と、

第２疑似ランダム信号発生回路の出力信号により、受信したデータを復号化する復号化回路とを具えている。

[作　用]

送信側及び受信側の第１及び第２疑似ランダム信号発生回路は、切り替え可能な帰還路を有するシフト・レジスタを用いている。よって、帰還路及び初期値を変更することにより、種々の異なる疑似ランダム信号を発生できる。

一方、第１及び第２記憶回路は、疑似ランダム信号発生回路の初期値及び帰還路設定データの組数を記憶している。よって、暗号鍵設定手段の設定に応じて、記憶回路の記憶内容を読出し、疑似ランダム信号発生回路を設定することにより、異なる疑似ランダム信号を発生できる。

すなわち、送信側では、第１疑似ランダム信号発生回路の疑似ランダム信号の種類は、暗号鍵設定手段の設定に応じたパラレル・アドレス信号により決まる。このパラレル・アドレス信号は、シ

リアル・アドレス信号に変換されて、送信側から受信側に伝送される。

受信側では、シリアル・アドレス信号をパラレル・アドレス信号に変換して、第2疑似ランダム信号発生回路の疑似ランダム信号を選択する。

よって、送信側及び受信側で、疑似ランダム信号が同じになり、暗号化されたデータを確実に復号化できる。

したがって、送信側の暗号鍵設定手段を変更するのみで、なんら受信側を変更することなく、暗号を変更できる。

[実施例]

以下、添付図を参照して、本発明の好適な実施例を説明する。

第1図は、送信側のブロック図である。疑似ランダム信号発生回路は、6段のシフト・レジスタSR1～SR6の縦続接続段1と、この縦続接続段1の帰還路を選択する切り替え回路2とで構成する。

縦続接続段1のシフト・レジスタのロード及びシフト状態は、制御手段であるマイクロコンピュータ6からの制御信号S/Lが制御する。この制御信号S/Lがロード状態のとき、シフト・レジスタSR1～SR6は、マイクロコンピュータ6からの初期値データPo1～Po6をロードする。なお、これらシフト・レジスタは、クロック信号CKに同期して動作する。

切り替え回路2は、種々のゲート及び反転器で構成されている。すなわち、アンド・ゲート21は、シフト・レジスタSR6の出力信号及びマイクロコンピュータ6からの制御信号Po7を受け、反転器22は、制御信号Po7を反転する。アンド・ゲート23は、シフト・レジスタSR1及び反転器22の出力を受け、オア・ゲート24は、アンド・ゲート21及び23の出力信号を受ける。よって、制御信号Po7が高か低かに応じて、シフト・レジスタSR1又はSR6の出力信号がオア・ゲート24の出力信号となる。

さらに、切り替え回路2では、排他的オア・ゲート25が、オア・ゲート24及びシフト・レジスタSRGの出力信号を受け、その排他的オアの結果をシフト・レジスタSR1に帰還している。

よって、シフト・レジスタSR1～SR6がシフト動作のとき、初期データ及び切り替え回路2の選択に応じた疑似ランダム信号が、シフト・レジスタSRGから発生する。

暗号鍵設定手段5は、接地（低）又は開放（高）を選択する6個のスイッチであり、その設定結果をマイクロコンピュータ6の端子PI1～PI6に供給する。

記憶回路であるリード・オンリ・メモリ（ROM）3は、縦続接続段1のシフト・レジスタの初期値と、切り替え回路2による帰還路設定データとを複数組記憶している。

マイクロコンピュータ6は、暗号鍵設定手段5の設定に応じてROM3をアドレス指定し、対応する初期値及び帰還路設定データを受け、制御信号Po1～Po7を発生して、疑似ランダム信号発生回路を設定する。

また、マイクロコンピュータ6は、暗号鍵設定手段5の設定に応じて、端子Po8～Po14にパラレル・アドレス信号を発生する。第1変換回路4は、マイクロコンピュータ6からのパラレル・アドレス信号をシリアル・アドレス信号に変換して出力する。

暗号化回路であるスクランブル回路7を、排他的オア・ゲートで構成する。このゲートは、疑似ランダム信号発生回路からの疑似ランダム信号と、データ発生手段（図示せず）からのシリアル・データ（例えば、音声データ）との排他的オアの結果を、暗号文として出力する。

データ/制御信号切り替え回路8は、変換回路4からのシリアル・アドレス信号（ROMアドレス指定用制御信号）、スクランブル回路7からの暗号文データ（音声データ）、及び同期信号発生回路9からの同期信号を、マイクロコンピュータ6の制御により、クロック信号に同期して切り替え、有線又は無線の通信回線に出力する。この際のタイミング例を第3図に示す。

このようにして、第1図の送信側では、暗号鍵

設定手段５の設定に応じて、データを暗号化し、同期信号及びＲＯＭアドレス指定用制御信号と共に、通信回線に出力する。

第２図は、受信側のブロック図である。第１図と同じブロックは、同じ参照番号で示し、異なる部分についてのみ、以下説明する。

データ／制御信号切り替え回路８は、通信回線からの信号を受け、この信号を同期信号検出回路１２に供給する。同期信号検出回路１２は、第３図に示すように、通信回線からの信号に含まれる同期信号を検出し、この検出結果を第２制御手段であるマイクロコンピュータ６に知らせる。

さらに、データ／制御信号切り替え回路８は、同期信号に応じたマイクロコンピュータ６からの制御信号Ｐｏ１７及びクロック信号に応じて、通信回線からのＲＯＭアドレス指定用制御信号（シリアル・アドレス信号）を第２変換回路１０に供給すると共に、暗号文データを復号化回路であるデスクランブル回路１１に供給する。

第２変換回路１０は、シリアル・アドレス信号をパラレル・アドレス信号に変換して、マイクロコンピュータ６の端子ＰＩ８～ＰＩ１４に供給する。マイクロコンピュータ６は、このアドレス信号に応じて、ＲＯＭ３から初期値及び帰還路設定データを読出し、縦続接続段１及び切り替え回路２の第２疑似ランダム信号発生回路を設定する。

受信側のＲＯＭ３の記憶内容は、送信側のＲＯＭ３の記憶内容と同じであり、受信側及び送信側の疑似ランダム信号発生回路は、同じ構成なので、受信側は、送信側と同じ疑似ランダム信号を発生する。

デスクランブル回路１１は、シフト・レジスタＳＲ６からの疑似ランダム信号、及びデータ／制御信号切り替え回路８からの暗号文データを受ける排他的オア・ゲートである。この構成は、送信側のスクランブル回路７と逆の構成であるので、暗号文データを平文データに変換できる。

上述は、本発明の好適な実施例について説明したが、本発明の要旨を逸脱することなく種々の変更ができる。例えば、縦続接続段のシフト・レジスタの段数は、任意の数でもよく、また、帰還路は、任意のシフト・レジスタの出力でもよい。

［発明の効果］

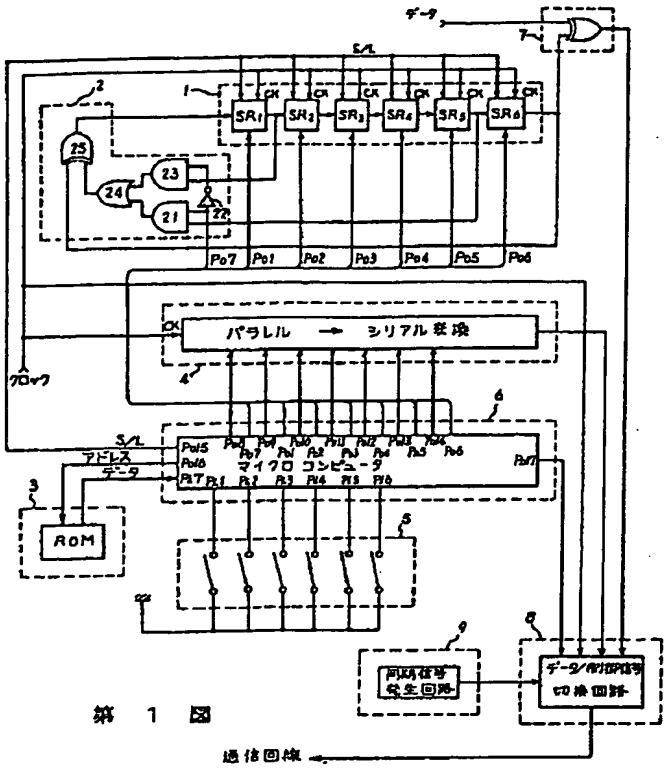
上述の如く、本発明の秘話装置によれば、送信側及び受信側にて、暗号鍵自体を取り替えることなく、容易且つ自由に鍵の設定及び変更が可能である。

4．図面の簡単な説明

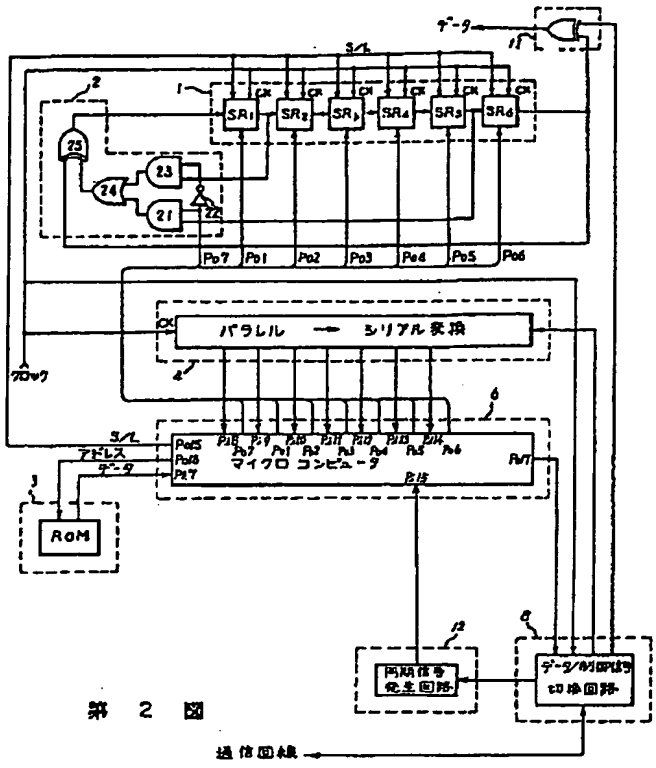
第１図は本発明による送信側のブロック図、第２図は本発明による受信側のブロック図、第３図は本発明による通信区間のタイミング図、第４図は従来の秘話装置のブロック図である。

１，２・・・疑似ランダム信号発生回路
３・・・記憶回路
４，１０・・・変換回路
５・・・暗号鍵設定手段
６・・・制御手段
７・・・暗号化回路
８・・・データ／制御信号切り替え回路
１１・・・復号化回路

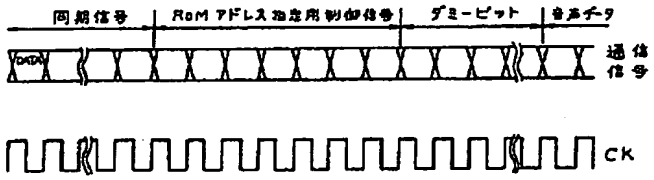
特許出願人　シャープ株式会社
代理人　弁理士　山口邦夫



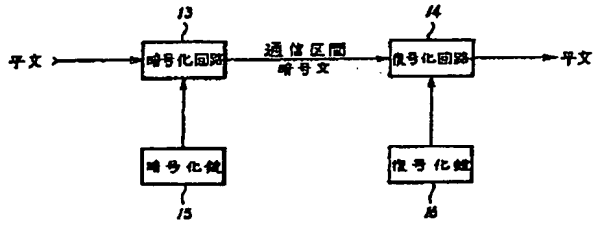
第 1 図



第 2 図



第 3 図



第 4 図